WE CLAIM

1. A proxy device for performing malware scanning of files stored within a file storage device of a computer network, the computer network having a plurality of client devices arranged to issue access requests using a dedicated file access protocol to the file storage device in order to access files stored on the file storage device, the proxy device being arranged so as to intercept access requests issued to the file storage device, and comprising:

a first interface for receiving an access request issued by one of said client devices to said file storage device using the dedicated file access protocol;

a second interface for communicating with the file storage device to cause the file storage device to process the access request;

processing logic for causing selected malware scanning algorithms to be executed to determine whether the file identified by the access request is to be considered as malware.

2. A proxy device as claimed in Claim 1, wherein the dedicated file access protocol is the Server Message Block (SMB) protocol, and the access requests are SMB calls issued to the file storage device.

3. A proxy device as claimed in Claim 1, wherein the dedicated file access protocol is the Network File System (NFS) protocol, and the access requests are NFS calls issued to the file storage device.

4. A proxy device as claimed in Claim 1, wherein each device in the computer network is assigned an identifier, and the proxy device is assigned the same identifier as is assigned to the file storage device, the first interface being connectable to a communication infrastructure of the computer network to enable communication between the proxy device and said client devices, and the file storage device being connectable to the second interface such that the file storage device is only accessible by said client devices via said proxy device.

5. A proxy device as claimed in Claim 4, wherein the second interface is configured to enable a plurality of file storage devices to be connected to the proxy device, each file storage device having a different identifier, and the proxy device being assigned multiple identifiers corresponding to the identifiers of the connected file storage devices, the first interface being configured to receive any access requests issued to one of said connected file storage devices.

6. A proxy device as claimed in Claim 1, wherein each device in the computer network is assigned an identifier, the proxy device being assigned a unique identifier different to the identifier of the file storage device, the client devices, the proxy device and the file storage device being connectable to a communication infrastructure of the computer network, the client devices being configured such that access requests issued by the client devices are routed to the proxy device, and the file storage device being configured to send processed access requests to the proxy device.

7. A proxy device as claimed in Claim 1, wherein the processing logic is responsive to configuration data to determine which malware scanning algorithms should be selected for a particular file, the proxy device further comprising a scanning engine to execute the malware scanning algorithms selected by the processing logic.

8. A proxy device as claimed in Claim 1, further comprising a file cache for storing files previously accessed by the client devices, upon receipt of an access request identifying a file to be read from the file storage device, the processing logic being arranged to determine whether the file identified by the access request is stored in the file cache and if so to return the file to the client device without communicating with the file storage device via the second interface.

9. A proxy device as claimed in Claim 8, wherein the file cache is arranged only to store files which have been determined not to be considered as malware.

10. A proxy device as claimed in Claim 1, wherein, upon receipt of an access request from a client device, the processing logic is arranged to determine from the access request predetermined attributes, and to send those predetermined attributes to the file storage device to enable the file storage device to perform a validation check, the processing logic only allowing the access request to proceed if the file storage device confirms that the client device is allowed to access the file identified by the file access request.

11. A proxy device as claimed in Claim 10, further comprising a user cache for storing the predetermined attributes.

12. A balanced proxy system for performing malware scanning of files stored within a file storage device of a computer network, the computer network having a plurality of client devices arranged to issue access requests using a dedicated file access protocol to the file storage device in order to access files stored on the file storage device, the balanced proxy system comprising:

a plurality of proxy devices as claimed in Claim 1 arranged so as to intercept access requests issued to the file storage device; and

a passive load balancing mechanism arranged to configure each client device to communicate with a particular proxy device in said plurality, such that an access request issued by a particular client device will be directed to a predetermined one of said proxy devices dependent on how that client device was configured by the passive load balancing mechanism.

13. A method of operating a proxy device to perform malware scanning of files stored within a file storage device of a computer network, the computer network having a plurality of client devices arranged to issue access requests using a dedicated file access protocol to the file storage device in order to access files stored on the file storage device, the proxy device being arranged so as to intercept access requests issued to the file storage device, and the method comprising the steps of:

(a) receiving an access request issued by one of said client devices to said file storage device using the dedicated file access protocol;

(b) communicating with the file storage device to cause the file storage device to process the access request; and

(c) causing selected malware scanning algorithms to be executed to determine whether the file identified by the access request is to be considered as malware.

14. A method as claimed in Claim 13, wherein the dedicated file access protocol is the Server Message Block (SMB) protocol, and the access requests are SMB calls issued to the file storage device.

15. A method as claimed in Claim 13, wherein the dedicated file access protocol is the Network File System (NFS) protocol, and the access requests are NFS calls issued to the file storage device.

16. A method as claimed in Claim 13, wherein each device in the computer network is assigned an identifier, and the proxy device is assigned the same identifier as is assigned to the file storage device, the method comprising the steps of:

connecting a first interface of the proxy device to a communication infrastructure of the computer network to enable communication between the proxy device and said client devices; and

connecting the file storage device to a second interface of the proxy device such that the file storage device is only accessible by said client devices via said proxy device.

17. A method as claimed in Claim 16, wherein the second interface is configured to enable a plurality of file storage devices to be connected to the proxy device, each file storage device having a different identifier, and the proxy device being assigned multiple identifiers corresponding to the identifiers of the connected file storage devices, the first interface being configured to receive any access requests issued to one of said connected file storage devices.

18. A method as claimed in Claim 13, wherein each device in the computer network is assigned an identifier, the proxy device being assigned a unique identifier different to the identifier of the file storage device, the method comprising the steps of:

connecting the client devices, the proxy device and the file storage device to a communication infrastructure of the computer network;

configuring the client devices such that access requests issued by the client devices are routed to the proxy device; and

configuring the file storage device to send processed access requests to the proxy device.

19. A method as claimed in Claim 13, wherein said step (c) comprises the steps of:

responsive to configuration data, determining which malware scanning algorithms should be selected for a particular file; and

employing a scanning engine to execute the malware scanning algorithms selected by said determining step.

20. A method as claimed in Claim 13, further comprising the steps of:

storing within a file cache files previously accessed by the client devices;

upon receipt of an access request identifying a file to be read from the file storage device, determining whether the file identified by the access request is stored in the file cache and if so returning the file to the client device without communicating with the file storage device.

21. A method as claimed in Claim 20, wherein the file cache is arranged only to store files which have been determined not to be considered as malware.

22. A method as claimed in Claim 13, further comprising the steps of:

upon receipt of an access request from a client device, determining from the access request predetermined attributes;

sending those predetermined attributes to the file storage device to enable the file storage device to perform a validation check; and

only allowing the access request to proceed if the file storage device confirms that the client device is allowed to access the file identified by the file access request.

23. A method as claimed in Claim 22, further comprising the step of storing within a user cache the predetermined attributes.

24. A method as claimed in Claim 13, wherein a plurality of said proxy devices are provided, the method further comprising the step of employing a passive load balancing mechanism to configure each client device to communicate with a particular proxy device in said plurality, such that an access request issued by a particular client device will be directed to a predetermined one of said proxy devices dependent on how that client device was configured by the passive load balancing mechanism.

25. A computer program product operable to configure a proxy device to perform a method of malware scanning of files stored within a file storage device of a computer network, the computer network having a plurality of client devices arranged to issue access requests using a dedicated file access protocol to the file storage device in order to access files stored on the file storage device, the proxy device being arranged so as to intercept access requests issued to the file storage device, and the computer program product comprising:

(a) reception code operable to receive an access request issued by one of said client devices to said file storage device using the dedicated file access protocol;

(b) communication code operable to communicate with the file storage device to cause the file storage device to process the access request; and

(c) algorithm invoking code operable to cause selected malware scanning algorithms to be executed to determine whether the file identified by the access request is to be considered as malware.

26. A computer program product as claimed in Claim 25, wherein the dedicated file access protocol is the Server Message Block (SMB) protocol, and the access requests are SMB calls issued to the file storage device.

27. A computer program product as claimed in Claim 25, wherein the dedicated file access protocol is the Network File System (NFS) protocol, and the access requests are NFS calls issued to the file storage device.

28. A computer program product as claimed in Claim 25, wherein each device in the computer network is assigned an identifier, and the proxy device is assigned the same identifier as is assigned to the file storage device, a first interface of the proxy device being connectable to a communication infrastructure of the computer network to enable communication between the proxy device and said client devices, and a second interface of the proxy device being connectable to the file storage device such that the file storage device is only accessible by said client devices via said proxy device.

29. A computer program product as claimed in Claim 28, wherein the second interface is configured to enable a plurality of file storage devices to be connected to the proxy device, each file storage device having a different identifier, and the proxy device being assigned multiple identifiers corresponding to the identifiers of the connected file storage devices, the reception code being operable to receive via the first interface any access requests issued to one of said connected file storage devices.

30. A computer program product as claimed in Claim 25, wherein each device in the computer network is assigned an identifier, the proxy device being assigned a unique identifier different to the identifier of the file storage device, the client devices, the proxy device and the file storage device being connectable to a communication infrastructure of the computer network, the client devices being configured such that access requests issued by the client devices are routed to the proxy device, and the file storage device being configured to send processed access requests to the proxy device.

31. A computer program product as claimed in Claim 25, wherein said algorithm invoking code is operable to determine, responsive to configuration data, which malware scanning algorithms should be selected for a particular file, and the computer

program product further comprises scanning engine code responsive to said algorithm invoking code and operable to execute the malware scanning algorithms selected by said algorithm invoking code.

32. A computer program product as claimed in Claim 25, further comprising:

caching code operable to store within a file cache files previously accessed by the client devices;

the reception code being operable, upon receipt of an access request identifying a file to be read from the file storage device, to determine whether the file identified by the access request is stored in the file cache and if so to cause the file to be returned to the client device without the communication code communicating with the file storage device.

33. A computer program product as claimed in Claim 32, wherein the file cache is arranged only to store files which have been determined not to be considered as malware.

34. A computer program product as claimed in Claim 25, wherein said reception code is operable, upon receipt of an access request from a client device, to determine from the access request predetermined attributes, the communication code being operable to send those predetermined attributes to the file storage device to enable the file storage device to perform a validation check, the access request only being allowed to proceed if the file storage device confirms that the client device is allowed to access the file identified by the file access request.

35. A computer program product as claimed in Claim 34, further comprising storing code operable to store within a user cache the predetermined attributes.

36. A computer program product as claimed in Claim 25, wherein a plurality of said proxy devices are provided, the computer program product further comprising passive load balancing code operable to configure each client device to communicate

with a particular proxy device in said plurality, such that an access request issued by a particular client device will be directed to a predetermined one of said proxy devices dependent on how that client device was configured by the passive load balancing code.